CYCLIC COVERS OF PRIME POWER DEGREE, JACOBIANS AND ENDOMORPHISMS

YURI G. ZARHIN

Abstract. Suppose K is a field of characteristic zero, K_a is its algebraic closure, $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$, whose Galois group coincides either with the full symmetric group $\mathbf{S}_n$ or with the alternating group $\mathbf{A}_n$. Let q be a power prime, $\mathcal{P}_q(t) = \frac{t^q-1}{t-1}$.

Let C be the superelliptic curve $y^q = f(x)$ and $J(C)$ its jacobian. We prove that if p does not divide n then the algebra $\mathrm{End}(J(C)) \otimes \mathbf{Q}$ of K_a-endomorphisms of $J(C)$ is canonically isomorphic to $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t]$.

1. Introduction

We write $\mathbf{Z}, \mathbf{Q}, \mathbf{C}$ for the ring of integers, the field of rational numbers and the field of complex numbers respectively. Recall that a number field is called a CM-field if it is a purely imaginary quadratic extension of a totally real field. Let p be a prime, $q = p^r$ an integral power of p, $\zeta_q \in \mathbf{C}$ a primitive qth root of unity, $\mathbf{Q}(\zeta_q) \subset \mathbf{C}$ the qth cyclotomic field and $\mathbf{Z}[\zeta_q]$ the ring of integers in $\mathbf{Q}(\zeta_q)$. If $q = 2$ then $\mathbf{Q}(\zeta_q) = \mathbf{Q}$. It is well-known that if $q > 2$ then $\mathbf{Q}(\zeta_q)$ is a CM-field of degree $(p-1)p^{r-1}$. Let us put

$$\mathcal{P}_q(t) = \frac{t^q - 1}{t-1} = t^{q-1} + \cdots + 1 \in \mathbf{Z}[t].$$

Clearly,

$$\mathcal{P}(t) = \prod_{i=1}^{r} \Phi_{p^i}(t)$$

where

$$\Phi_{p^i}(t) = t^{(p-1)p^{i-1}} + \cdots + t^{p^{i-1}} + 1 \in \mathbf{Z}[t]$$

is the p^ith cyclotomic polynomial. In particular,

$$\mathbf{Q}[t]/\Phi_{p^i}(t)\mathbf{Q}[t] = \mathbf{Q}(\zeta_{p^i})$$

and

$$\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^{r} \mathbf{Q}(\zeta_{p^i}).$$

We write $\mathbf{F}_p$ for the finite field with p elements.

Let $f(x) \in \mathbf{C}[x]$ be a polynomial of degree $n \ge 4$ without multiple roots. Let $C_{f,q}$ be a smooth projective model of the smooth affine curve

$$y^q = f(x).$$

Throughout this paper we assume that either p does not divide n or q divides n. It is well-known that the genus $g(C_{f,q})$ of $C_{f,q}$ is $(q-1)(n-1)/2$ if p does not divide n and $(q-1)(n-2)/2$ if q divides n. The map

$$(x,y) \mapsto (x, \zeta_q y)$$

gives rise to a non-trivial birational automorphism

$$\delta_q : C_{f,q} \to C_{f,q}$$

of period q.

The jacobian $J(C_{f,q})$ of $C_{f,q}$ is an abelian variety of dimension $g(C_{f,q})$. We write $\mathrm{End}(J^{(f,q)})$ for the ring of endomorphisms of $J^{(f,p)}$ over $\mathbf{C}$ and $\mathrm{End}^0(J(C_{f,q}))$ for the endomorphism algebra $\mathrm{End}(J(C_{f,q})) \otimes \mathbf{Q}$. By Albanese functoriality, δ_q induces an automorphism of $J(C_{f,q})$ which we still denote by δ_q. One may easily check (see 4.8 below) that

$$\delta_q^{q-1} + \cdots + \delta_q + 1 = 0$$

in $\mathrm{End}(J(C_{f,q}))$. This implies that if $\mathbf{Q}[\delta_q]$ is the $\mathbf{Q}$-subalgebra of $\mathrm{End}^0(J(C_{f,q}))$ generated by δ_q then there is the natural surjective homomorphism

$$\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] \twoheadrightarrow \mathbf{Q}[\delta_q]$$

which sends $t + \mathcal{P}_q(t)\mathbf{Q}[t]$ to δ_q. One may check that this homomorphism is, in fact, an isomorphism (see [9, p. 149], [10, p. 458]) where the case $q = p$ was treated).

This gives us an embedding

$$\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] \cong \mathbf{Q}[\delta_q] \subset \mathrm{End}^0(J(C_{f,q})).$$

Our main result is the following statement.

Theorem 1.1. *Let K be a subfield of $\mathbf{C}$ such that all the coefficients of $f(x)$ lie in K. Assume also that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \ge 5$ and its Galois group over K is either the symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. In addition, assume that either p does not divide n or $q \mid n$. Then*

$$\mathrm{End}^0(J(C_{f,q})) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^{r} \mathbf{Q}(\zeta_{p^i}).$$

Remark 1.2. In the case when q is a prime (i.e. $q = p$) the assertion of Theorem 1.1 is proven in [16, 23]. See [21, 25, 20] for a discussion of finite characteristic case.

Examples 1.3. Let $n \ge 5$ be an integer, p a prime, r a positive integer, $q = p^r$.

(1) The polynomial $x^n - x - 1 \in \mathbf{Q}[x]$ has Galois group $\mathbf{S}_n$ over $\mathbf{Q}$ ([13, p. 42]). Therefore the endomorphism algebra (over $\mathbf{C}$) of the jacobian $J(C)$ of the curve $C : y^q = x^n - x - 1$ is $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t]$.

(2) The Galois group of the "truncated exponential"

$$\exp_n(x) := 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots + \frac{x^n}{n!} \in \mathbf{Q}[x]$$

is either $\mathbf{S}_n$ or $\mathbf{A}_n$ [11]. Therefore the endomorphism algebra (over $\mathbf{C}$) of the jacobian $J(C)$ of the curve $C : y^q = \exp_n(x)$ is $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t]$.

Remark 1.4. If $f(x) \in K[x]$ then the curve $C_{f,q}$ and its jacobian $J(C_{f,q})$ are defined over K. Let $K_a \subset \mathbf{C}$ be the algebraic closure of K. Clearly, all endomorphisms of $J(C_{f,q})$ are defined over K_a. This implies that in order to prove Theorem 1.1, it suffices to check that $\mathbf{Q}[\delta_q]$ coincides with the $\mathbf{Q}$-algebra of K_a-endomorphisms of $J(C_{f,q})$.

2. Complex abelian varieties

Throughout this section we assume that Z is a complex abelian variety of positive dimension. As usual, we write $\mathrm{End}^0(Z)$ for the semisimple finite-dimensional $\mathbf{Q}$-algebra $\mathrm{End}(Z) \otimes \mathbf{Q}$. We write $\mathfrak{C}_Z$ for the center of $\mathrm{End}^0(Z)$. It is well-known that $\mathfrak{C}_Z$ is a direct product of finitely many number fields. All the fields involved are either totally real number fields or CM-fields. Let $H_1(Z, \mathbf{Q})$ be the first rational homology group of Z; it is a $2\dim(Z)$-dimensional $\mathbf{Q}$-vector space. By functoriality, $\mathrm{End}^0(Z)$ acts on $H_1(Z, \mathbf{Q})$; hence we have an embedding

$$\mathrm{End}^0(Z) \hookrightarrow \mathrm{End}_{\mathbf{Q}}(H_1(Z, \mathbf{Q}))$$

(which sends 1 to 1).

Suppose E is a subfield of $\mathrm{End}^0(Z)$ that contains the identity map. Then $H_1(Z, \mathbf{Q})$ becomes an E-vector space of dimension

$$d = \frac{2\dim(Z)}{[E : \mathbf{Q}]}.$$

We write

$$\mathrm{Tr}_E : \mathrm{End}_E(H_1(Z, \mathbf{Q})) \to E$$

for the corresponding trace map on the E-algebra of E-linear operators in $H_1(Z,\mathbf{Q})$.

Extending by $\mathbf{C}$-linearity the action of $\mathrm{End}^0(Z)$ and of E on the complex cohomology group

$$H_1(Z,\mathbf{Q})\otimes_{\mathbf{Q}}\mathbf{C}=H_1(Z,\mathbf{C})$$

of Z we get the embeddings

$$E\otimes_{\mathbf{Q}}\mathbf{C}\subset \mathrm{End}^0(Z)\otimes_{\mathbf{Q}}\mathbf{C}\hookrightarrow \mathrm{End}_{\mathbf{C}}(H_1(Z,\mathbf{C}))$$

which provide $H_1(Z,\mathbf{C})$ with a natural structure of free $E_{\mathbf{C}}:=E\otimes_{\mathbf{Q}}\mathbf{C}$-module of rank d. If Σ_E is the set of all field embeddings $\sigma: E\hookrightarrow\mathbf{C}$ then it is well-known that

$$E_{\mathbf{C}}=E\otimes_{\mathbf{Q}}\mathbf{C}=\prod_{\sigma\in\Sigma_E}E\otimes_{E,\sigma}\mathbf{C}=\prod_{\sigma\in\Sigma_E}\mathbf{C}_\sigma$$

where

$$\mathbf{C}_\sigma=E\otimes_{E,\sigma}\mathbf{C}=\mathbf{C}.$$

Since $H_1(Z,\mathbf{C})$ is a free $E_{\mathbf{C}}$-module of rank d, there is the corresponding trace map

$$\mathrm{Tr}_{E_{\mathbf{C}}}:\mathrm{End}_{E_{\mathbf{C}}}(H_1(Z,\mathbf{C}))\to E_{\mathbf{C}}$$

which coincides on $E_{\mathbf{C}}$ with multiplication by d and with Tr_E on $\mathrm{End}_E(H_1(Z,\mathbf{Q}))$.

We write $\mathrm{Lie}(Z)$ for the tangent space of Z; it is a $\dim(Z)$-dimensional $\mathbf{C}$-vector space. By functoriality, $\mathrm{End}^0(Z)$ and therefore E act on $\mathrm{Lie}(Z)$. This provides $\mathrm{Lie}(Z)$ with a natural structure of $E\otimes_{\mathbf{Q}}\mathbf{C}$-module. We have

$$\mathrm{Lie}(Z)=\bigoplus_{\sigma\in\Sigma_E}\mathbf{C}_\sigma\mathrm{Lie}(Z)=\oplus_{\sigma\in\Sigma_E}\mathrm{Lie}(Z)_\sigma$$

where

$$\mathrm{Lie}(Z)_\sigma=\mathbf{C}_\sigma\mathrm{Lie}(Z)=\{x\in\mathrm{Lie}(Z)\mid ex=\sigma(e)x\quad\forall e\in E\}.$$

Let us put

$$n_\sigma=n_\sigma(Z,E)=\dim_{\mathbf{C}_\sigma}\mathrm{Lie}(Z)_\sigma=\dim_{\mathbf{C}}\mathrm{Lie}(Z)_\sigma.$$

Remark 2.1. Let $\Omega^1(Z)$ be the space of the differentials of the first kind on Z. It is well-known that the natural map

$$\Omega^1(Z)\to\mathrm{Hom}_{\mathbf{C}}(\mathrm{Lie}(Z),\mathbf{C})$$

is an isomorphism. This isomorphism allows us to define via duality the natural homomorphism

$$E\to\mathrm{End}_{\mathbf{C}}(\mathrm{Hom}_{\mathbf{C}}(\mathrm{Lie}(Z),\mathbf{C}))=\mathrm{End}_{\mathbf{C}}(\Omega^1(Z)).$$

This provides $\Omega^1(Z)$ with a natural structure of $E \otimes_{\mathbf{Q}} \mathbf{C}$-module in such a way that

$$\Omega^1(Z)_\sigma := \mathbf{C}_\sigma \Omega^1(Z) \cong \mathrm{Hom}_{\mathbf{C}}(\mathrm{Lie}(Z)_\sigma, \mathbf{C}).$$

In particular,

$$n_\sigma = \dim_{\mathbf{C}}(\mathrm{Lie}(Z)_\sigma) = \dim_{\mathbf{C}}(\Omega^1(Z)_\sigma).$$

Theorem 2.2. *Suppose that E contains $\mathfrak{C}_Z$. Then the tuple*

$$(n_\sigma)_{\sigma \in \Sigma_E} \in \prod_{\sigma \in \Sigma_E} \mathbf{C}_\sigma = E \otimes_{\mathbf{Q}} \mathbf{C}$$

lies in $\mathfrak{C}_Z \otimes_{\mathbf{Q}} \mathbf{C}$. In particular, if $E/\mathbf{Q}$ is Galois and $\mathfrak{C}_Z \neq E$ then there exists a nontrivial automorphism $\kappa : E \to E$ such that $n_\sigma = n_{\sigma\kappa}$ for all $\sigma \in \Sigma_E$.

Proof. This is Theorem 2.3 of [23]. □

Corollary 2.3. *Suppose that there exist a prime p, a positive integer r, the power prime $q = p^r$ and an integer $n \geq 4$ enjoying the following properties:*

(i) *$E = \mathbf{Q}(\zeta_q) \subset \mathbf{C}$ where $\zeta_q \in \mathbf{C}$ is a primitive qth root of unity;*

(ii) *n is not divisible by p, i.e. n and q are relatively prime:*

(iii) *Let $i < q$ be a positive integer that is not divisible by p and $\sigma_i : E = \mathbf{Q}(\zeta_q) \hookrightarrow \mathbf{C}$ an embedding that sends ζ_q to ζ_q^{-i}. Then*

$$n_{\sigma_i} = \left[\frac{ni}{q}\right].$$

Then $\mathfrak{C}_Z = \mathbf{Q}(\zeta_q)$.

Proof. If $q = 2$ then $E = \mathbf{Q}(\zeta_2) = \mathbf{Q}$. Since $\mathfrak{C}_Z$ is a subfield of $E = \mathbf{Q}$, we conclude that $\mathfrak{C}_Z = \mathbf{Q} = \mathbf{Q}(\zeta_2)$.

So, further we assume that $q > 2$. Clearly, $\{\sigma_i\}$ is the collection Σ of all embeddings $\mathbf{Q}(\zeta_q) \hookrightarrow \mathbf{C}$. It is also clear that $n_{\sigma_i} = 0$ if and only if $1 \leq i \leq [\frac{q}{n}]$. Suppose that $\mathfrak{C}_Z \neq \mathbf{Q}(\zeta_q)$. It follows from Theorem 2.2 that there exists a non-trivial field automorphism $\kappa : \mathbf{Q}[\zeta_q] \to \mathbf{Q}[\zeta_q]$ such that for all $\sigma \in \Sigma$

$$n_\sigma = n_{\sigma\kappa}.$$

Clearly, there exists an integer m such that p does *not* divide m, $1 < m < q$ and $\kappa(\zeta_q) = \zeta_q^m$.

Assume that $q < n$. In this case the function $i \mapsto n_{\sigma_i} = [\frac{ni}{q}]$ is strictly increasing and therefore $n_{\sigma_i} \neq n_{\sigma_j}$ while $i \neq j$. This implies that $\sigma_i = \sigma_i\kappa$, i.e. κ is the identity map which is not the case. The obtained contradiction implies that

$$n < q.$$

Since $n \ge 4$,

$$q \ge 5.$$

Clearly, $n_\sigma = 0$ if and only if $\sigma = \sigma_i$ with $1 \le i \le [\frac{q}{n}]$. Since n and q are relatively prime, $[\frac{q}{n}] = [\frac{q-1}{n}]$. It follows that $n_{\sigma_i} = 0$ if and only if $1 \le i \le [\frac{q-1}{n}]$. Clearly, the map $\sigma \mapsto \sigma\kappa$ permutes the set $\{\sigma_i \mid 1 \le i \le [\frac{(q-1)}{n}], p \text{ does not divide } i\}$. Since $\kappa(\zeta_q) = \zeta_q^m$, $\sigma_i\kappa(\zeta_q) = \zeta_q^{-im}$. This implies that multiplication by m in $(\mathbf{Z}/q\mathbf{Z})^* = \mathrm{Gal}(\mathbf{Q}(\zeta_q)/\mathbf{Q})$ leaves invariant the subset

$$A := \{i \bmod q \in \mathbf{Z}/q\mathbf{Z} \mid 1 \le i \le [\frac{(q-1)}{n}], p \text{ does not divide } i\}.$$

Clearly, A contains 1 and therefore $m = m \cdot 1 \in A$. Since $m < q$,

$$m = m \cdot 1 \le \left[\frac{(q-1)}{n}\right] \le \frac{(q-1)}{4}.$$

Let us consider the arithmetic progression consisting of $2m$ integers $[\frac{(q-1)}{n}] + 1, \dots, [\frac{(q-1)}{n}] + 2m$ with difference 1. All its elements lie between $[\frac{(q-1)}{n}] + 1$ and

$$\left[\frac{(q-1)}{n}\right] + 2m \le 3\left[\frac{(q-1)}{n}\right] \le 3\frac{(q-1)}{4} < q - 1.$$

Clearly, there exist exactly two elements of A say, d_1 and $d_2 = d_1 + m$ that are divisible by m. Then there is a positive integer c_1 such that

$$d_1 = mc_1, d_2 = m(c_1 + 1).$$

Clearly, either c_1 or $c_1 + 1$ is not divisible by p; we put $c = c_1$ in the former case and $c = c_1 + 1$ in the latter case. However, c is not divisible by p and

$$\left[\frac{(q-1)}{n}\right] < mc \le \left[\frac{(q-1)}{n}\right] + 2m < q - 1.$$

In particular, mc does not lie in A. It follows that c also does not lie in A and therefore

$$c > \left[\frac{(q-1)}{n}\right].$$

This means that

$$mc > m\left[\frac{(q-1)}{n}\right].$$

Since

$$mc \le \left[\frac{(q-1)}{n}\right] + 2m,$$

we conclude that

$$(m-1)\left[\frac{(q-1)}{n}\right] < 2m$$

and therefore

$$\left[\frac{(q-1)}{n}\right] < \frac{2m}{m-1} = 2 + \frac{2}{m-1}.$$

Since

$$1 < m < \left[\frac{(q-1)}{n}\right],$$

we conclude that if $m > 2$ then $m \geq 3$ and

$$3 \leq m < \left[\frac{(q-1)}{n}\right] < 2 + \frac{2}{m-1} \leq 3$$

and therefore $3 < 3$ which could not be the case. Hence $m = 2$ and

$$2 = m < \left[\frac{(q-1)}{n}\right] < 2 + \frac{2}{m-1} = 4$$

and therefore

$$\left[\frac{(q-1)}{n}\right] = 3.$$

It follows that

$$q \geq 1 + 3n \geq 1 + 3 \cdot 4 = 13.$$

Since $m = 2$ is not divisible by p, we conclude that $p \geq 3$ and either $p = 3$ and $A = \{1, 2\}$ or $p > 3$ and $A = \{1, 2, 3\}$. In both cases $4 = 2 \cdot 2 = m \cdot 2$ must lie in A. Contradiction. □

3. Abelian varieties over arbitrary fields

Let K be a field. Let us fix its algebraic closure K_a and denote by $\mathrm{Gal}(K)$ the absolute Galois group $\mathrm{Aut}(K_a/K)$ of K. If X is an abelian variety over K_a then we write $\mathrm{End}(X)$ for the ring of all its K_a-endomorphisms. We write 1_X (or even just 1) for the identity automorphism of X. If Y is (may be another) abelian variety over K_a then we write $\mathrm{Hom}(X, Y)$ for the group of all K_a-homomorphisms from X to Y. It is well-known that $\mathrm{Hom}(X, Y) = 0$ if and only if $\mathrm{Hom}(Y, X) = 0$. One may easily check that if X is simple and $\dim(X) \geq \dim(Y)$ then $\mathrm{Hom}(X, Y) = 0$ if and only if X and Y are *not* isogenous over K_a. We write $\mathrm{End}^0(X)$ for the finite-dimensional semisimple $\mathbf{Q}$-algebra $\mathrm{End}(X) \otimes \mathbf{Q}$ and $\mathrm{Hom}^0(X, Y)$ for the finite-dimensional $\mathbf{Q}$-vector space $\mathrm{Hom}(X, Y) \otimes \mathbf{Q}$. Clearly, if $X = Y$ then

$$\mathrm{End}^0(X) = \mathrm{Hom}^0(X, Y) = \mathrm{Hom}^0(Y, X) = \mathrm{End}^0(Y).$$

It is well-known that $\mathrm{Hom}^0(X, Y)$ and $\mathrm{Hom}^0(Y, X)$ have the same dimension which does not exceed $4\dim(X)\dim(Y)$ [6]. The equality holds if and only if $\mathrm{char}(K) > 0$ and both X and Y are supersingular abelian varieties [16, 22].

It is well-known that if X and Y are simple and the $\mathbf{Q}$-algebras $\mathrm{End}^0(X)$ and $\mathrm{End}^0(Y$ are *not* isomorphic then

$$\mathrm{Hom}(X,Y)=0,\ \mathrm{Hom}(Y,X)=0.$$

Let E be a number field and $\emptyset \subset E$ be the ring of all its algebraic integers. Let (X,i) be a pair consisting of an abelian variety X over K_a and an embedding

$$i : E \hookrightarrow \mathrm{End}^0(X)$$

Here $1 \in E$ must go to 1_X. It is well known [7] that the degree $[E : \mathbf{Q}]$ divides $2\dim(X)$, i.e.

$$r = r_X := \frac{2\dim(X)}{E : \mathbf{Q}]}$$

is a positive integer.

Let us denote by $\mathrm{End}^0(X,i)$ the centralizer of $i(E)$ in $\mathrm{End}^0(X)$. Clearly, $i(E)$ lies in the center of the finite-dimensional $\mathbf{Q}$-algebra $\mathrm{End}^0(X,i)$. It follows that $\mathrm{End}^0(X,i)$ carries a natural structure of finite-dimensional E-algebra. If Y is (possibly) another abelian variety over K_a and $j : E \hookrightarrow \mathrm{End}^0(Y)$ is an embedding that sends 1 to the identity automorphism of Y then we write

$$\mathrm{Hom}^0((X,i),(Y,j)) = \{u \in \mathrm{Hom}^0(X,Y) \mid ui(c) = j(c)u \quad \forall c \in E\}.$$

Clearly, $\mathrm{End}^0(X,i) = \mathrm{Hom}^0((X,i),(X,i))$. If d is a positive integer then we write $i^{(d)}$ for the composition

$$E \hookrightarrow \mathrm{End}^0(X) \subset \mathrm{End}^0(X^d)$$

of i and the diagonal inclusion $\mathrm{End}^0(X) \subset \mathrm{End}^0(X^d)$.

Remark 3.1. (i) The E-algebra $\mathrm{End}^0(X,i)$ is semisimple. Indeed, let us split the semisimple $\mathbf{Q}$-algebra $\mathrm{End}^0(X)$ into a finite direct product

$$\mathrm{End}^0(X) = \prod_s D_s$$

of simple $\mathbf{Q}$-algebras D_s. If $\mathrm{pr}_s : \mathrm{End}^0(X) \twoheadrightarrow D_s$ is the corresponding projection map and $D_{s,E}$ is the centralizer of $\mathrm{pr}_s i(E)$ in D_s then one may easily check that

$$\mathrm{End}^0(X,i) = \prod_s D_{s,E}.$$

Clearly, $\mathrm{pr}_s i(E) \cong E$ is a simple $\mathbf{Q}$-algebra. It follows from Theorem 4.3.2 on p. 104 of [1] that $D_{s,E}$ is also a *simple* $\mathbf{Q}$-algebra. This implies easily that $D_{s,E}$ is a *simple* E-algebra and therefore $\mathrm{End}^0(X,i)$ is a semisimple

E-algebra. It is also clear that $\mathrm{End}^0(X,i)$ is a simple E-algebra if and only if $\mathrm{End}^0(X)$ is a simple $\mathbf{Q}$-algebra, i.e., X is isogenous to a self-product of (absolutely) simple abelian variety.

(ii) Let e_s be the identity element of D_s. One may view e_s as an idempotent in $\mathrm{End}^0(X)$. Clearly,

$$1 = \sum_s e_s$$

in $\mathrm{End}^0(X)$ and $e_s e_t = 0$ if $s \neq t$. There exists a positive integer N such that all $N \cdot e_s$ lie in $\mathrm{End}(X)$. We write X_s for the image

$$X_s := (Ne_s)(X);$$

it is an abelian subvariety in X of positive dimension. Clearly, the sum map

$$\pi_X : \prod_s X_s \to X, \quad (x_s) \mapsto \sum_s x_s$$

is an isogeny. It is also clear that the intersection $D_s \bigcap \mathrm{End}(X)$ leaves $X_s \subset X$ invariant. This gives us a natural identification

$$D_s \cong \mathrm{End}^0(X_s).$$

One may easily check that each X_s is isogenous to a self-product of (absolutely) simple abelian variety. It is also clear that

$$\mathrm{Hom}(X_s, X_t) = 0 \quad \forall s \neq t.$$

We write i_s for the composition

$$\mathrm{pr}_s i : E \hookrightarrow \mathrm{End}^0(X) \twoheadrightarrow D_s \cong \mathrm{End}^0(X_s).$$

Clearly,

$$D_{s,E} = \mathrm{End}^0(X_s, i_s)$$

and

$$\pi_X^{-1} i \pi_X = \prod_s i_s : E \to \prod_s D_s = \prod_s \mathrm{End}^0(X_s) \subset \mathrm{End}^0(\prod_s X_s).$$

It is also clear that

$$\mathrm{End}^0(\prod_s X_s, \prod_s i_s) = \prod_s D_{s,E}.$$

Theorem 3.2. (i)

$$\dim_E(\mathrm{End}^0((X,i)) \leq \frac{4 \cdot \dim(X)^2}{[E:\mathbf{Q}]^2};$$

(ii) *Suppose that*

$$\dim_E(\mathrm{End}^0((X,i)) = \frac{4\cdot \dim(X)^2}{[E:\mathbf{Q}]^2}.$$

Then X is isogenous to a self-product of (absolutely) simple abelian variety. Also $\mathrm{End}^0((X,i)$ is a central simple E-algebra, i.e., E coincides with the center of $\mathrm{End}^0((X,i)$. In addition, X is an abelian variety of CM-type.

If $\mathrm{char}(K_a) = 0$ then $[E:\mathbf{Q}]$ is even and there exist a $\frac{[E:\mathbf{Q}]}{2}$-dimensional abelian variety Z, an isogeny $\psi : Z^r \to X$, an embedding

$$k : E \hookrightarrow \mathrm{End}^0(Z)$$

that sends 1 to 1_Z and such that

$$\psi \in \mathrm{Hom}^0((Z^r, k^{(r)}), (X,i)).$$

Proof. Recall that $r = 2\dim(X)/[E:\mathbf{Q}]$.

First, assume that X is isogenous to a self-product of (absolutely) simple abelian variety, i.e., $\mathrm{End}^0(X,i)$ is a simple E-algebra. We need to prove that

$$N := \dim_E(\mathrm{End}^0(X,i)) \le r^2.$$

Let E' be the center of $\mathrm{End}^0(X,i)$. Let us put

$$e = [E' : E].$$

Then $\mathrm{End}^0(X,i)$ is a *central* simple E'-algebra of dimension N/e. Then there exists a central division E'-algebra D such that $\mathrm{End}^0(X,i)$ is isomorphic to the matrix algebra $\mathrm{M}_m(D)$ of size m for some positive integer m. Dimension arguments imply that

$$m^2 \dim_{E'}(D) = \frac{N}{e}, \quad \dim_{E'}(D) = \frac{N}{em^2}.$$

Since $\dim_{E'}(D)$ is a square,

$$\frac{N}{e} = N_1^2, \quad N = eN_1^2, \quad \dim_{E'}(D) = \left(\frac{N_1}{m}\right)^2$$

for some positive integer N_1. Clearly, m divides N_1.

Clearly, D contains a (maximal) field extension L/E' of degree $\frac{N_1}{m}$ and $\mathrm{End}^0(X,i) \cong \mathrm{M}_m(D)$ contains every field extension T/L of degree m. This implies that

$$\mathrm{End}^0(X) \supset \mathrm{End}^0(X,i) \supset T$$

and the number field T has degree

$$[T:\mathbf{Q}] = [E':\mathbf{Q}] \cdot \frac{N_1}{m} \cdot m = [E:\mathbf{Q}]eN_1.$$

But $[T:\mathbf{Q}]$ must divide $2\dim(X)$; if the equality holds then X is an abelian variety of CM-type. This implies that eN_1 divides $r = \frac{2\dim(X)}{[E:\mathbf{Q}]}$. It follows that $(eN_1)^2$ divides r^2; if the equality holds then X is an abelian variety of CM-type. But

$$(eN_1)^2 = e^2N_1^2 = e(eN_1^2) = eN = e \cdot \dim_E(\mathrm{End}^0(X,i)).$$

This implies that

$$\dim_E(\mathrm{End}^0(X,i)) \le \frac{r^2}{e} \le r^2.$$

If the equality $\dim_E(\mathrm{End}^0(X,i)) = r^2$ holds then $e=1$ and

$$(eN_1)^2 = r^2, N_1 = r,\ [T:\mathbf{Q}] = [E:\mathbf{Q}]eN_1 = [E:\mathbf{Q}]r = 2\dim(X);$$

in particular, X is an abelian variety of CM-type. In addition, since $e=1$, we have $E' = E$, i.e. $\mathrm{End}^0(X,i)$ is a central simple E-algebra.

Clearly, there exists an abelian variety Z over K_a with

$$E \subset D \subset \mathrm{End}^0(Z)$$

and an isogeny

$$\psi : Z^m \to X$$

such that the induced isomorphism

$$\mathrm{End}^0(Z^m) \cong \mathrm{End}^0(X),\ u \mapsto \psi u \psi^{-1}$$

maps identically

$$E \subset \mathrm{End}^0(Z) \subset \mathrm{End}^0(Z^m)$$

onto $E \subset \mathrm{End}^0(X)$.

We still have to check that if $\mathrm{char}(K) = 0$ then

$$2\dim(Z) = [E:\mathbf{Q}].$$

Indeed, since D is a division algebra, $\dim_{\mathbf{Q}}(D)$ must divide $2\dim(Z) = \frac{2\dim(X)}{m} = [E:\mathbf{Q}]\frac{r}{m}$. On the other hand,

$$\dim_{\mathbf{Q}}(D) = [E:\mathbf{Q}]\dim_E(D) = [E:\mathbf{Q}]\left(\frac{r}{m}\right)^2.$$

Since m divides r, we conclude that $\frac{r}{m} = 1$, i.e.

$$\dim_E(D) = 1, \quad D = E, \quad 2\dim(Z) = [E:\mathbf{Q}].$$

Now let us consider the case of arbitrary X. Applying the already proven case of the theorem to each X_s, we conclude that

$$\dim_E(\mathrm{End}^0(X,i)) \le \left(\frac{2\dim(X_s)}{[E:\mathbf{Q}]}\right)^2.$$

Since

$$\mathrm{End}^0(X,i) = \prod_s \mathrm{End}^0(X_s,i_s),$$

we conclude that $\dim_E(\mathrm{End}^0(X,i)) = \sum_s \dim_E(\mathrm{End}^0(X_s,i_s))$ does not exceed

$$\sum_s \left(\frac{2\dim(X_s)}{[E:\mathbf{Q}]}\right)^2 \le \frac{(2\sum_s \dim(X_s))^2}{[E:\mathbf{Q}]^2} = \frac{(2\dim(X))^2}{[E:\mathbf{Q}]^2}.$$

It follows that if the equality

$$\dim_E(\mathrm{End}^0(X,i)) = \frac{(2\dim(X))^2}{[E:\mathbf{Q}]^2}$$

holds then the set of indices s is a singleton, i.e. $X = X_s$ is isogenous to a self-product of (absolutely) simple abelian variety. □

Let d be a positive integer that is not divisible by $\mathrm{char}(K)$. Let X be an abelian variety of positive dimension defined over K. We write X_d for the kernel of multiplication by d in $X(K_a)$. It is known [6] that the commutative group X_d is a free $\mathbf{Z}/d\mathbf{Z}$-module of rank $2\dim(X)$. Clearly, X_d is a Galois submodule in $X(K_a)$. We write

$$\tilde{\rho}_{d,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{Z}/d\mathbf{Z}}(X_d) \cong \mathrm{GL}(2\dim(X), \mathbf{Z}/d\mathbf{Z})$$

for the corresponding (continuous) homomorphism defining the Galois action on X_d. Let us put

$$\tilde{G}_{d,X} = \tilde{\rho}_{d,X}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{\mathbf{Z}/d\mathbf{Z}}(X_d).$$

Clearly, $\tilde{G}_{d,X}$ coincides with the Galois group of the field extension $K(X_d)/K$ where $K(X_d)$ is the field of definition of all points on X of order dividing d. In particular, if a prime $\ell \ne \mathrm{char}(K)$ then X_ℓ is a $2\dim(X)$-dimensional vector space over the prime field $\mathbf{F}_\ell = \mathbf{Z}/\ell\mathbf{Z}$ and the inclusion $\tilde{G}_{\ell,X} \subset \mathrm{Aut}_{\mathbf{F}_\ell}(X_\ell)$ defines a faithful linear representation of the group $\tilde{G}_{\ell,X}$ in the vector space X_ℓ.

We write $\mathrm{End}_K(X) \subset \mathrm{End}(X)$ for the (sub)ring of all K-endomorphisms of X.

Now let us assume that

$$i(\emptyset) \subset \mathrm{End}_K(X).$$

Let λ be a maximal ideal in $\mathcal{O}$. We write $k(\lambda)$ for the corresponding (finite) residue field. Let us put

$$X_\lambda := \{x \in X(K_a) \mid i(e)x = 0 \quad \forall e \in \lambda\}.$$

Clearly, if $\mathrm{char}((k)(\lambda)) = \ell$ then $\lambda \supset \ell \cdot \mathcal{O}$ and therefore $X_\lambda \subset X_\ell$. Clearly, X_λ is a Galois submodule of X_ℓ. It is also clear that X_λ carries a natural structure of $\mathcal{O}/\lambda = k(\lambda)$-vector space. We write

$$\tilde{\rho}_{\lambda,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{k(\lambda)}(X_\lambda)$$

for the corresponding (continuous) homomorphism defining the Galois action on X_λ. Let us put

$$\tilde{G}_{\lambda,X} = \tilde{G}_{\lambda,i,X} := \tilde{\rho}_{\lambda,X}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{k(\lambda)}(X_\lambda).$$

Clearly, $\tilde{G}_{\lambda,X}$ coincides with the Galois group of the field extension $K(X_\lambda)/K$ where $K(X_\lambda) = K(X_{\lambda,i})$ is the field of definition of all points in X_λ.

In order to describe $\tilde{\rho}_{\lambda,X}$ explicitly, let us assume for the sake of simplicity that λ is the only maximal ideal of $\mathcal{O}$ dividing ℓ, i.e.,

$$\ell \cdot \mathcal{O} = \lambda^b$$

where the positive integer b satisfies

$$[E : \mathbf{Q}] = b \cdot [k(\lambda) : \mathbf{F}_\ell].$$

Then $\mathcal{O} \otimes \mathbf{Z}_\ell = \mathcal{O}_\lambda$ where $\mathcal{O}_\lambda$ is the completion of $\mathcal{O}$ with respect to λ-adic topology. It is well-known that that $\mathcal{O}_\lambda$ is a local principal ideal domain and its only maximal ideal is $\lambda\mathcal{O}_\lambda$. One may easily check that $\ell \cdot \mathcal{O}_\lambda = (\lambda\mathcal{O}_\lambda)^b$.

Let us choose an element $c \in \lambda$ that does not lie in λ^2. Clearly, $\lambda\mathcal{O}_\lambda = c \cdot \mathcal{O}_\lambda$. This implies that there exists a unit $u \in \mathcal{O}_\lambda^*$ such that $\ell = uc^b$. It follows from the unique factorization of ideals in $\mathcal{O}$ that

$$\lambda = \ell \cdot \mathcal{O} + c \cdot \mathcal{O}.$$

It follows readily that

$$X_\lambda = \{x \in X_\ell \mid cx = 0\} \subset X_\ell.$$

Let $T_\ell(X)$ be the $\mathbf{Z}_\ell$-Tate module of X defined as projective limit of Galois modules X_{ℓ^m} where the transition map(s) $X_{\ell^{m+1}} \to X_{\ell^m}$ is multiplication by ℓ

[6]. Recall that $T_\ell(X)$ is a free $\mathbf{Z}_\ell$-module of rank $2\dim(X)$ provided with the continuous action

$$\rho_{\ell,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X))$$

and the natural embedding

$$\mathrm{End}_K(X) \otimes \mathbf{Z}_\ell \hookrightarrow \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell(X)),$$

whose image commutes with $\rho_{\ell,X}(\mathrm{Gal}(K))$. In particular, $T_\ell(X)$ carries the natural structure of $\emptyset \otimes \mathbf{Z}_\ell = \emptyset_\lambda$-module; it is known [7] that the $\emptyset_\lambda$-module $T_\ell(X)$ is free of rank $r = r_X = \frac{2\dim(X)}{[E:\mathbf{Q}]}$. There is also the natural isomorphism of Galois modules

$$X_\ell = T_\ell(X)/\ell T_\ell(X),$$

which is also an isomorphism of $\mathrm{End}_K(X) \supset \emptyset$-modules. This implies that the $\emptyset[\mathrm{Gal}(K)]$-module X_λ coincides with

$$c^{-1}\ell T_\ell(X)/\ell T_\ell(X) = c^{b-1}T_\ell(X)/c^b T_\ell(X) = T_\ell(X)/cT_\ell(X) =$$

$$T_\ell(X)/\lambda T_\ell(X) = T_\ell(X)/(\lambda\emptyset_\lambda)T_\ell(X).$$

Hence

$$X_\lambda = T_\ell(X)/(\lambda\emptyset_\lambda)T_\ell(X) = T_\ell(X) \otimes_{\emptyset_\lambda} k(\lambda).$$

It follows that

$$\dim_{k(\lambda)} X_\lambda = \frac{2\dim(X)}{[E:\mathbf{Q}]} := r_X.$$

Let us put

$$V_\ell(X) = T_\ell(X) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell;$$

it is a $2\dim(X)$-dimensional $\mathbf{Q}_\ell$-vector space that carries a natural structure of r_X-dimensional E_λ-vector space. There is the natural embedding

$$\mathrm{End}(X) \otimes \mathbf{Z}_\ell \hookrightarrow \mathrm{End}_{\mathbf{Q}_\ell} V_\ell(X).$$

Extending it by $\mathbf{Q}$-linearity, we get the natural embedding

$$\mathrm{End}^0(X) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbf{Q}_\ell}(V_\ell(X)).$$

Further we will identify $\mathrm{End}^0(X) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ with its image in $\mathrm{End}_{\mathbf{Q}_\ell}(V_\ell(X))$.

Remark 3.3. Notice that

$$E_\lambda = E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell = \emptyset \otimes \mathbf{Q}_\ell = \emptyset_\lambda \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$$

is the field coinciding with the completion of E with respect to λ-adic topology. Clearly, $V_\ell(X)$ carries a natural structure of r_X-dimensional E_λ-vector space. One

may easily check that $\mathrm{End}^0(X,i)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell$ is a $E\otimes_{\mathbf{Q}}\mathbf{Q}_\ell = E_\lambda$-vector subspace (even subalgebra) in $\mathrm{End}_{E_\lambda}(V_\ell(X))$. Clearly,

$$\dim_{E_\lambda}(\mathrm{End}^0(X,i)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell) = \dim_E(\mathrm{End}^0(X,i))$$

and

$$\dim_{E_\lambda}(\mathrm{End}_{E_\lambda}(V_\ell(X))) = r_X^2.$$

This implies that

$$\mathrm{End}^0(X,i)\otimes_{\mathbf{Q}}\mathbf{Q}_\ell = \mathrm{End}_{E_\lambda}(V_\ell(X))$$

if and only if

$$\dim_E(\mathrm{End}^0(X,i)) = r_X^2.$$

Using the inclusion

$$\mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X)) \subset \mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(X)),$$

one may view $\rho_{\ell,X}$ as ℓ-adic representation

$$\rho_{\ell,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{Z}_\ell}(T_\ell(X)) \subset \mathrm{Aut}_{\mathbf{Q}_\ell}(V_\ell(X)).$$

Since X is defined over K, one may associate with every $u \in \mathrm{End}(X)$ and $\sigma \in \mathrm{Gal}(K)$ an endomorphism ${}^\sigma u \in \mathrm{End}(X)$ such that

$${}^\sigma u(x) = \sigma u(\sigma^{-1}x) \quad \forall x \in X(K_a).$$

Clearly,

$${}^\sigma u = u \quad \forall u \in \mathrm{End}_K(X).$$

In particular,

$${}^\sigma u = u \quad \forall u \in \emptyset$$

(here we identify $\emptyset$ with $i(\emptyset)$). It follows easily that for each $\sigma \in \mathrm{Gal}(K)$ the map $u \to {}^\sigma u$ extends by $\mathbf{Q}$-linearity to a certain automorphism of $\mathrm{End}^0(X)$. It is also clear that ${}^\sigma u = u$ for each $u \in E$ and

$${}^\sigma u \in \mathrm{End}^0(X,i) \quad \forall u \in \mathrm{End}^0(X,i), \sigma \in \mathrm{Gal}(K).$$

Remark 3.4. The definition of $T_\ell(X)$ as the projective limit of Galois modules X_{ℓ^m} implies that

$${}^\sigma u(x) = \rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1}(x) \quad \forall x \in T_\ell(X).$$

It follows easily that

$${}^\sigma u(x) = \rho_{\ell,X}(\sigma)u\rho_{\ell,X}(\sigma)^{-1}(x) \quad \forall x \in V_\ell(X), u \in \mathrm{End}^0(X), \sigma \in \mathrm{Gal}(K).$$

This implies that for each $\sigma \in \mathrm{Gal}(K)$

$$\rho_{\ell,X}(\sigma) \in \mathrm{Aut}_{E_\lambda}(V_\lambda(X)).$$

and therefore

$$\rho_{\ell,X}(\mathrm{Gal}(K)) \subset \mathrm{Aut}_{E_\lambda}(V_\lambda(X))$$

[12, 7]. It is also clear that

$$\rho_{\ell,X}(\sigma) u \rho_{\ell,X}(\sigma)^{-1} \in \mathrm{End}^0(X) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \quad \forall u \in \mathrm{End}^0(X) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$$

and

$$\rho_{\ell,X}(\sigma) u \rho_{\ell,X}(\sigma)^{-1} \in \mathrm{End}^0(X,i) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \quad \forall u \in \mathrm{End}^0(X,i) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell.$$

We refer to [17, 18, 21, 24] for a discussion of the following definition.

Definition 3.5. Let V be a vector space over a field $\mathbf{F}$, let G be a group and $\rho : G \to \mathrm{Aut}_{\mathbf{F}}(V)$ a linear representation of G in V. We say that the G-module V is *very simple* if it enjoys the following property:

If $R \subset \mathrm{End}_{\mathbf{F}}(V)$ is an $\mathbf{F}$-subalgebra containing the identity operator Id such that

$$\rho(\sigma) R \rho(\sigma)^{-1} \subset R \quad \forall \sigma \in G$$

then either $R = \mathbf{F} \cdot \mathrm{Id}$ or $R = \mathrm{End}_{\mathbf{F}}(V)$.

Remarks 3.6.

(i) If G' is a subgroup of G and the G'-module V is very simple then obviously the G-module V is also very simple.

(ii) Clearly, the G-module V is very simple if and only if the corresponding $\rho(G)$-module V is very simple. This implies easily that if $H \twoheadrightarrow G$ is a surjective group homomorphism then the G-module V is very simple if and only if the corresponding H-module V is very simple.

(iii) Let G' be a normal subgroup of G. If V is a very simple G-module then either $\rho(G') \subset \mathrm{Aut}_k(V)$ consists of scalars (i.e., lies in $k \cdot \mathrm{Id}$) or the G'-module V is absolutely simple. See [21, Remark 5.2(iv)].

(iv) Suppose F is a discrete valuation field with valuation ring O_F, maximal ideal m_F and residue field $k = O_F/m_F$. Suppose V_F a finite-dimensional F-vector space, $\rho_F : G \to \mathrm{Aut}_F(V_F)$ a F-linear representation of G. Suppose T is a G-stable O_F-lattice in V_F and the corresponding $k[G]$-module $T/m_F T$ is isomorphic to V. Assume that the G-module V is very simple. Then the G-module V_F is also very simple. See [21, Remark 5.2(v)].

Theorem 3.7. *Suppose that X is an abelian variety defined over K and $i(\mathcal{O}) \subset \mathrm{End}_K(X)$. Let ℓ be a prime different from $\mathrm{char}(K)$. Suppose that λ is the only maximal ideal dividing ℓ in $\mathcal{O}$. Suppose that the natural representation in the $k(\lambda)$-vector space X_λ is very simple. Then $\mathrm{End}^0(X,i)$ enjoy one of the following two properties:*

(i) $\mathrm{End}^0(X,i) = i(E)$, *i.e.* $i(E) \cong E$ *is a maximal commutative subalgebra in* $\mathrm{End}^0(X)$ *and* $i(\mathcal{O}) \cong \mathcal{O}$ *is a maximal commutative subring in* $\mathrm{End}(X)$*;*

(ii) $\mathrm{End}^0(X,i)$ *is a central simple E-algebra of dimension r_X^2 and X is an abelian variety of CM-type over K_a. In addition, if* $\mathrm{char}(K) = 0$ *then* $[E:\mathbf{Q}]$ *is even and there exist a $\frac{[E:\mathbf{Q}]}{2}$-dimensional abelian variety Z, an isogeny $\psi : Z^r \to X$ and an embedding*

$$k : E \hookrightarrow \mathrm{End}^0(Z)$$

that sends 1 *to* 1_Z *such that*

$$\psi \in \mathrm{Hom}^0((Z^r, k^{(r)}), (X,i)).$$

Proof. In light of 3.6(ii), the $\mathrm{Gal}(K)$-module X_λ is very simple. In light of 3.6(iv) and Remark 3.4

$$\rho_{\ell,X} : \mathrm{Gal}(K) \to \mathrm{Aut}_{E_\lambda}(V_\ell(X))$$

is also very simple. Let us put

$$R = \mathrm{End}^0(X,i) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell.$$

It follows from Remark 3.4 that either $R = E_\lambda \mathrm{Id}$ or $R = \mathrm{End}_{E_\lambda}(V_\ell(X))$. By Remark 3.3,

$$\dim_{E_\lambda}(R) = \dim_{E_\lambda}(\mathrm{End}^0(X,i) \otimes_{\mathbf{Q}} \mathbf{Q}_\ell) = \dim_E(\mathrm{End}^0(X,i)).$$

It follows that $\dim_E(\mathrm{End}^0(X,i)) = 1$ or r_X^2. Clearly, if $\dim_E(\mathrm{End}^0(X,i)) = 1$ then $\mathrm{End}^0(X,i) = i(E)$ and the property (i) holds. Suppose that $\dim_E(\mathrm{End}^0(X,i)) = r_X^2$. Applying Theorem 3.2, we conclude that the property (ii) holds. □

Let Y be an abelian variety of positive dimension over K_a and u a non-zero endomorphism of Y. Let us consider the abelian (sub)variety

$$Z = u(Y) \subset Y.$$

Remark 3.8. If Y is defined over K and $u \in \mathrm{End}_K(Y)$ then Z is also defined over K and the inclusion map $Z \subset Y$ is defined over K. Indeed, clearly, Z and the inclusion map $Z \subset Y$ are defined over $K_a^{\mathrm{Gal}(K)}$, i.e. Z and $Z \subset Y$ are defined over a purely inseparable extension of K. By Theorem of Chow [3, Th. 5 on p. 26], Z is defined over K. It follows that every homomorphism between Z and Y is defined over a separable extension of K. Hence $Z \subset Y$ is defined over K.

We write $\Omega^1(Y)$ (resp. $\Omega^1(Z)$) for the $\dim(Y)$-dimensional (resp. $\dim(Z)$-dimensional) K_a-vector space of differentials of the first kind on Y (resp. on Z).

Theorem 3.9. *Let Y be an abelian variety of positive dimension over K_a and δ an automorphism of Y. Suppose that the induced K_a-linear operator*

$$\delta^* : \Omega^1(Y) \to \Omega^1(Y)$$

is diagonalizable. Let S be the set of eigenvalues of δ^* and $\mathrm{mult}_Y : S \to \mathbf{Z}_+$ the integer-valued function which assigns to each eigenvalue its multiplicity.

Suppose that $P(t)$ is a polynomial with integer coefficients such that $u = P(\delta)$ is a non-zero endomorphism of Y. Let us put $Z = u(Y)$. Clearly, Z is δ-invariant and we write $\delta_Z : Z \to Z$ for the corresponding automorphism of Z (i.e. for the restriction of δ to z). Suppose that

$$\dim(Z) = \sum_{\lambda \in S, P(\lambda) \neq 0} \mathrm{mult}_Y(\lambda).$$

Then the spectrum of $\delta_Z^* : \Omega^1(Z) \to \Omega^1(Z)$ coincides with $S_P = \{\lambda \in S, P(\lambda) \neq 0\}$ and the multiplicity of an eigenvalue λ of δ_Z^* equals $mult_Y(\lambda)$.

Proof. Clearly, u commutes with δ. We write v for the (surjective) homomorphism $Y \twoheadrightarrow Z$ induced by u and j for the inclusion map $Z \subset Y$. Notice that $u : Y \to Y$ splits into a composition

$$Y \stackrel{v}{\twoheadrightarrow} Z \stackrel{j}{\hookrightarrow} Y,$$

i.e. $u = jv$. Clearly,

$$\delta_Z v = v\delta \in \mathrm{Hom}(Y, Z), \quad j\delta_Z = \delta j \in \mathrm{Hom}(Z, Y), \quad u = jv \in \mathrm{End}(Y), \quad u\delta = \delta u \in \mathrm{End}(Y).$$

It is also clear that the induced map

$$u^* : \Omega^1(Y) \to \Omega^1(Y)$$

coincides with $P(\delta^*)$. It follows that

$$u^*(\Omega^1(Y)) = P(\delta^*)(\Omega^1(Y))$$

has dimension

$$\sum_{\lambda\in S, P(\lambda)\neq 0} \mathrm{mult}_Y(\lambda) = \dim(Y)$$

and coincides with

$$\oplus_{\lambda\in S, P(\lambda)\neq 0} W_\lambda$$

where W_λ is the eigenspace of δ attached to eigenvalue λ. Since $u^* = v^* j^*$,

$$u^*(\Omega^1(Y)) = v^* j^*(\Omega^1(Y)) \subset v^*(\Omega^1(Z)).$$

Since

$$\dim(u^*(\Omega^1(Y))) = \dim(Y) = \dim(\Omega^1(Z)) \geq \dim(v^*(\Omega^1(Z))),$$

the subspace

$$u^*(\Omega^1(Y)) = v^*(\Omega^1(Z))$$

and

$$v^* : \Omega^1(Z) \hookrightarrow \Omega^1(Y).$$

It follows that if we denote by w the isomorphism $v^* : \Omega^1(Z) \cong v^*(\Omega^1(Z))$ and by γ the restriction of δ^* to $v^*(\Omega^1(Z))$ then $\gamma w = w\delta_Y^*$ and therefore

$$\gamma = w\delta_Y^* w^{-1}.$$

□

4. Cyclic covers and jacobians

Throughout this paper we fix a prime number p and its integral power $q = p^r$ and assume that K is a field of characteristic different from p. We fix an algebraic closure K_a and write $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Aut}(K_a/K)$. We also fix in K_a a primitive qth root of unity ζ.

Let $f(x) \in K[x]$ be a separable polynomial of degree $n \geq 4$. We write $\mathfrak{R}_f$ for the set of its roots and denote by $L = L_f = K(\mathfrak{R}_f) \subset K_a$ the corresponding splitting field. As usual, the Galois group $\mathrm{Gal}(L/K)$ is called the Galois group of f and denoted by $\mathrm{Gal}(f)$. Clearly, $\mathrm{Gal}(f)$ permutes elements of $\mathfrak{R}_f$ and the natural map of $\mathrm{Gal}(f)$ into the group $\mathrm{Perm}(\mathfrak{R}_f)$ of all permutations of $\mathfrak{R}_f$ is an embedding. We will identify $\mathrm{Gal}(f)$ with its image and consider it as a permutation group of $\mathfrak{R}_f$. Clearly, $\mathrm{Gal}(f)$ is transitive if and only if f is irreducible in $K[x]$.

Further, we assume that either p does not divide n or q does divide n.

If p does not divide n then we write (as in [19])

$$V_{f,p} = (\mathbf{F}_p^{\mathfrak{R}_f})^{00} = (\mathbf{F}_p^{\mathfrak{R}_f})^0$$

for the $(n-1)$-dimensional $\mathbf{F}_p$-vector space of functions

$$\phi : \mathfrak{R}_f \to \mathbf{F}_p, \ \sum_{\alpha \in \mathfrak{R}_f} \phi(\alpha) = 0\}$$

provided with a natural action of the permutation group $\mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f)$. It is the *heart* over the field $\mathbf{F}_p$ of the group $\mathrm{Gal}(f)$ acting on the set $\mathfrak{R}_f$ [5, 19].

Remark 4.1. If p does not divide n and $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$ then the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple.

Let $C = C_{f,q}$ be the smooth projective model of the smooth affine K-curve

$$y^q = f(x).$$

So C is a smooth projective curve defined over K. The rational function $x \in K(C)$ defines a finite cover $\pi : C \to \mathbf{P}^1$ of degree p. Let $B' \subset C(K_a)$ be the set of ramification points. Clearly, the restriction of π to B' is an *injective* map $B' \hookrightarrow \mathbf{P}^1(K_a)$, whose image is the disjoint union of ∞ and $\mathfrak{R}_f$ if p does *not* divide $\deg(f)$ and just $\mathfrak{R}_f$ if it does. We write

$$B = \pi^{-1}(\mathfrak{R}_f) = \{(\alpha, 0) \mid \alpha \in \mathfrak{R}_f\} \subset B' \subset C(K_a).$$

Clearly, π is ramified at each point of B with ramification index q. We have $B' = B$ if and only if n is divisible by p. If n is not divisible by p then B' is the disjoint union of B and a single point $\infty' := \pi^{-1}(\infty)$. In addition, the ramification index of π at $\pi^{-1}(\infty)$ is also q. Using Hurwitz's formula, one may easily compute the genus $g = g(C) = g(C_{q,f})$ of C ([2, pp. 401–402], [14, proposition 1 on p. 3359], [9, p. 148]). Namely, g is $(q-1)(n-1)/2$ if p does *not* divide n and $(q-1)(n-2)/2$ if q does divide n.

Remark 4.2. Assume that p does not divide n and consider the plane triangle (Newton polygon)

$$\Delta_{n,q} := \{(j,i) \mid 0 \le j, \quad 0 \le i, \quad qj + ni \le nq\}$$

with the vertices $(0,0)$, $(0,q)$ and $(n,0)$. Let $L_{n,q}$ be the set of integer points in the interior of $\Delta_{n,q}$. One may easily check that $g = (q-1)(n-1)/2$ coincides with the number of elements of $L_{n,q}$. It is also clear that for each $(j,i) \in L_{n,q}$

$$1 \le j \le n-1; \quad 1 \le i \le q-1; \quad q(j-1) + (j+1) \le n(q-i).$$

Elementary calculations ([2, theorem 3 on p. 403]) show that

$$\omega_{j,i} := x^{j-1}dx/y^{q-i} = x^{j-1}y^i dx/y^q = x^{j-1}y^{i-1}dx/y^{q-1}$$

is a differential of the first kind on C for each $(j,i) \in L_{n,q}$. This implies easily that the collection $\{\omega_{j,i}\}_{(j,i)\in L_{n,q}}$ is a basis in the space of differentials of the first kind on C.

There is a non-trivial birational K_a-automorphism of C

$$\delta_q : (x,y) \mapsto (x, \zeta y).$$

Clearly, δ_q^q is the identity map and the set of fixed points of δ_q coincides with B'.

Remark 4.3. Let us assume that $n = \deg(f)$ is divisible by q say, $n = qm$ for some positive integer m. Let $\alpha \in K_a$ be a root of f and $K_1 = K(\alpha)$ be the corresponding subfield of K_a. We have $f(x) = (x-\alpha)f_1(x)$ with $f_1(x) \in K_1[x]$. Clearly, $f_1(x)$ is a separable polynomial over K_1 of degree $qm - 1 = n - 1 \geq 4$. It is also clear that the polynomials

$$h(x) = f_1(x+\alpha), h_1(x) = x^{n-1}h(1/x) \in K_1[x]$$

are separable of the same degree $qm - 1 = n - 1 \geq 4$. The standard substitution

$$x_1 = 1/(x-\alpha), y_1 = y/(x-\alpha)^m$$

establishes a birational isomorphism between $C_{f,p}$ and a curve

$$C_{h_1} : y_1^q = h_1(x_1)$$

(see [14, p. 3359]). In particular, the jacobians of C_f and C_{h_1} are isomorphic over K_a (and even over K_1). But $\deg(h_1) = qm - 1$ is *not* divisible by p. Clearly, this isomorphism commutes with the actions of δ_q. Notice also that if the Galois group of f over K is $\mathbf{S}_n$ (resp. $\mathbf{A}_n$) then the Galois group of h_1 over K_1 is SS_{n-1} (resp. $\mathbf{A}_{n-1}$).

Remark 4.4. (i) Let $\Omega^1(C) = \Omega^1(C_{(f,q)})$ be the K-vector space of differentials of the first kind on C. It is well-known that $\dim_K(\Omega^1(C_{(f,q)}))$ coincides with the genus of $C_{(f,q)}$. By functoriality, δ_q induces on $\Omega^1(C_{(f,q)})$ a certain K-linear automorphism

$$\delta_q^* : \Omega^1(C_{(f,q)}) \to \Omega^1(C_{(f,q)}).$$

Clearly, if for some positive integer j the differential $\omega_{j,i} = x^{j-1}dx/y^{q-i}$ lies in $\Omega^1(C_{(f,q)})$ then it is an eigenvector of δ_q^* with eigenvalue ζ^i.

(ii) Now assume that p does *not* divide n. It follows from Remark 4.2 that the collection

$$\{\omega_{j,i} = x^{j-1}dx/y^{q-i} \mid (i,j) \in L_{n,q}\}$$

is an eigenbasis of $\Omega^1(C_{(f,q)})$. This implies that the multiplicity of the eigenvalue ζ^{-i} of δ_q^* coincides with number of interior integer points in $\Delta_{n,q}$ along the corresponding (to $q-i$) horizontal line. Elementary calculations show that this number is $\left[\frac{ni}{q}\right]$; in particular, ζ^{-i} *is an eigenvalue if and only if* $\left[\frac{ni}{q}\right] > 0$. Taking into account that $n \ge 4$ and $q = p^r$, we conclude that ζ^i is an eigenvalue of δ_q^* for each integer i with $p^r - p^{r-1} \le i \le p^r - 1 = q - 1$. It also follows easily that 1 is *not* an eigenvalue δ_q^*. This implies that

$$\mathcal{P}_q(\delta_q^*) = \delta_q^{*q-1} + \cdots + \delta_q^* + 1 = 0$$

in $\mathrm{End}_K(\Omega^1(C_{(f,q)}))$. In addition, one may easily check that if $\mathcal{H}(t)$ is a polynomial with rational coefficients such that $\mathcal{H}(\delta_q^*) = 0$ in $\mathrm{End}_K(\Omega^1(C_{(f,q)}))$ then $\mathcal{H}(t)$ is *divisible* by $\mathcal{P}_q(t)$ in $\mathbf{Q}[t]$.

Let $J(C_{f,q}) = J(C) = J(C_{f,q})$ be the jacobian of C. It is a g-dimensional abelian variety defined over K and one may view (via Albanese functoriality) δ_q as an element of

$$\mathrm{Aut}(C) \subset \mathrm{Aut}(J(C)) \subset \mathrm{End}(J(C))$$

such that $\delta_q \ne \mathrm{Id}$ but $\delta_q^q = \mathrm{Id}$ where Id is the identity endomorphism of $J(C)$. Here $\mathrm{Aut}(C)$ stands for the group of K_a-automorphisms of C, $\mathrm{Aut}(J(C))$ stands for the group of K_a-automorphisms of $J(C)$ and $\mathrm{End}(J(C))$ stands for the ring of all K_a-endomorphisms of $J(C)$. We write $\mathbf{Z}[\delta_q]$ for the subring of $\mathrm{End}(J(C))$ generated by δ_q. As usual, we write $\mathrm{End}^0(J(C)) = \mathrm{End}^0(J(C_{f,q}))$ for the corresponding $\mathbf{Q}$-algebra $\mathrm{End}(J(C)) \otimes \mathbf{Q}$. We write $\mathbf{Q}[\delta_q]$ for the $\mathbf{Q}$-subalgebra of $\mathrm{End}^0(J(C))$ generated by δ_q.

Remark 4.5. Assume that p does not divide n. Let P_0 be one of the δ_q-invariant points (i.e., a ramification point for π) of $C_{f,p}(K_a)$. Then

$$\tau : C_{f,q} \to J(C_{f,q}), \quad P \mapsto \mathrm{cl}((P) - (P_0))$$

is an embedding of complex algebraic varieties and it is well-known that the induced map

$$\tau^* : \Omega^1(J(C_{f,q})) \to \Omega^1(C_{f,q})$$

is a $\mathbf{C}$-linear isomorphism obviously commuting with the actions of δ_q. (Here cl stands for the linear equivalence class.) This implies that n_{σ_i} coincides with the dimension of the eigenspace of $\Omega^1(C_{(f,q)})$ attached to the eigenvalue ζ^{-i} of δ_q^*. Applying Remark 4.4, we conclude that if $\mathcal{H}(t)$ is a monic polynomial with integer coefficients such that $\mathcal{H}(\delta_q) = 0$ in $\mathrm{End}(J^{(f,q)})$ then $\mathcal{H}(t)$ is divisible by $\mathcal{P}_q(t)$ in $\mathbf{Q}[t]$ and therefore in $\mathbf{Z}[t]$.

Remark 4.6. Assume that p does not divide n. Clearly, the set S of eigenvalues λ of

$$\delta_q^* : \Omega^1(J(C_{f,q})) \to \Omega^1(J(C_{f,q}))$$

with $\mathcal{P}_{q/p}(\lambda) \neq 0$ consists of *primitive* qth roots of unity ζ^{-i} $(1 \leq i < q, (i,p) = 1)$ with $\left[\frac{ni}{q}\right] > 0$ and the multiplicity of ζ^{-i} equals $\left[\frac{ni}{q}\right]$, thanks to Remarks 4.5 and 4.4. Let us compute the sum

$$M = \sum_{1 \leq i < q, (i,p)=1} \left[\frac{ni}{q}\right]$$

of multiplicities of eigenvalues from S.

First, assume that $q > 2$. Then $\varphi(q) = (p-1)p^{r-1}$ is even and for each (index) i the difference $q - i$ is also prime to p, lies between 1 and q and

$$\left[\frac{ni}{q}\right] + \left[\frac{n(q-i)}{q}\right] = n - 1.$$

It follows easily that

$$M = (n-1)\frac{\varphi(q)}{2} = \frac{(n-1)(p-1)p^{r-1}}{2}.$$

Now assume that $q = p = 2$ and therefore $r = 1$. Then n is odd,

$$C_{f,q} = C_{f,2} : y^2 = f(x)$$

is a hyperelliptic curve of genus $g = \frac{n-1}{2}$ and

$$\delta_2 : (x, y) \mapsto (x, -y).$$

It is well-known that the differentials $x^i \frac{dx}{y}$ $(0 \leq i \leq g-1)$ constitute a basis of the g-dimensional $\Omega^1(J(C_{f,2}))$. It follows that δ_2^* is just multiplication by -1. Therefore

$$M = g = \frac{n-1}{2} = \frac{(n-1)(p-1)p^{r-1}}{2}.$$

Notice that if the abelian (sub)variety $Z := \mathcal{P}_{q/p}(\delta_q)(J(C_{f,q}))$ has dimension M then the data $Y = J(C_{f,q}), \delta = \delta_q, P = \mathcal{P}_{q/p}(t)$ satisfy the conditions of Theorem 3.9.

Lemma 4.7. *Assume that p does not divide n. Let $D = \sum_{P\in B} a_P(P)$ be a divisor on $C = C_{f,p}$ with degree 0 and support in B. Then D is principal if and only if all the coefficients a_P are divisible by q.*

Proof. Suppose $D = \mathrm{div}(h)$ where $h \in K_a(C)$ is a non-zero rational function of C. Since D is δ_q-invariant, the rational function

$$\delta_q^* h := h\delta_q = c \cdot h$$

for some non-zero $c \in K_a$. It follows easily from the δ_q-invariance of the splitting

$$K_a(C) = \oplus_{i=0}^{q-1} y^i \cdot K_a(x)$$

that

$$h = y^i \cdot u(x)$$

for some non-zero rational function $u(x) \in K_a(x)$ and a non-negative integer $i \le q-1$. It follows easily that all finite zeros and poles of $u(x)$ lie in B, i.e., there exists an integer-valued function b on $\mathfrak{R}_f$ such that u coincides, up to multiplication by a non-zero constant, to $\prod_{\alpha\in\mathfrak{R}_f}(x-\alpha)^{b(\alpha)}$. Notice that

$$\mathrm{div}(y) = \sum_{P\in B}(P) - n(\infty).$$

On the other hand, for each $\alpha \in \mathfrak{R}_f$, we have $P_\alpha = (\alpha, 0) \in B$ and the corresponding divisor

$$\mathrm{div}(x-\alpha) = q((\alpha,0)) - q(\infty) = q(P_\alpha) - q(\infty)$$

is divisible by q. This implies that

$$a_{P_\alpha} = q \cdot b(\alpha) + i.$$

Also, since ∞ is neither zero no pole of h,

$$0 = ni + \sum_{\alpha\in\mathfrak{R}_f} b(\alpha)q.$$

Since n and q are relatively prime, i must divide q. This implies that $i = 0$ and therefore the divisor

$$D = \mathrm{div}(u(x)) = \mathrm{div}(\prod_{\alpha\in\mathfrak{R}_f}(x-\alpha)^{b(\alpha)})$$

is divisible by q.

Conversely, suppose a divisor $D = \sum_{P\in B} a_P(P)$ with $\sum_{P\in B} a_P = 0$ and all a_P are divisible by q. Let us put

$$h = \prod_{P\in B} (x - x(P))^{a_P/q}.$$

One may easily check that $D = \mathrm{div}(h)$. □

Lemma 4.8. $1 + \delta_q + \cdots + \delta_q^{q-1} = 0$ *in* $\mathrm{End}(J(C_{f,q}))$. *The subring* $\mathbf{Z}[\delta_q] \subset \mathrm{End}(J(C_{f,q}))$ *is isomorphic to the ring* $\mathbf{Z}[t]/\mathcal{P}_q(t)\mathbf{Z}[t]$. *The* $\mathbf{Q}$*-subalgebra* $\mathbf{Q}[\delta_q] \subset \mathrm{End}^0(J(C_{f,q})) = \mathrm{End}^0(J(C_{f,q}))$ *is isomorphic to* $\mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

Proof. If $q = p$ is a prime this assertion is proven in [9, p. 149], [10, p. 458]. So, further we may assume that $q > p$. It follows from Remark 4.3 that we may assume that p does *not* divide n.

Now we follow arguments of [10, p. 458] (where the case of $q = p$ was treated). The group $J(C_{f,q}))(K_a)$ is generated by divisor classes of the form $(P) - (\infty)$ where P is a finite point on $C_{f,p}$. The divisor of the rational function $x - x(P)$ is $(\delta_q^{q-1}P) + \cdots + (\delta_q P) + (P) - q(\infty)$. This implies that

$$\mathcal{P}_q(\delta_q) = 0 \in \mathrm{End}(J(C_{f,q})).$$

Applying Remark 4.5(ii), we conclude that $\mathcal{P}_q(t)$ is the minimal polynomial of δ_q in $\mathrm{End}(J(C_{f,q}))$. □

Let us define the abelian (sub)variety

$$J^{(f,q)} := \mathcal{P}_{q/p}(\delta_q)(J(C_{f,q})) \subset J(C_{f,q}).$$

Clearly, $J^{(f,q)}$ is a δ_q-invariant abelian subvariety defined over $K(\zeta_q)$. In addition,

$$\Phi_q(\delta_q)(J^{(f,q)}) = 0.$$

Remark 4.9. If $q = p$ then $\mathcal{P}_{q/p}(t) = \mathcal{P}_1(t) = 1$ and therefore $J^{(f,p)} = J(C_{f,p})$.

Remark 4.10. Since the polynomials Φ_q and $\mathcal{P}_{q/p}$ are relatively prime, the homomorphism

$$\mathcal{P}_{q/p}(\delta_q) : J^{(f,q)} \to J^{(f,q)}$$

has finite kernel and therefore is an isogeny. In particular, it is surjective.

Lemma 4.11. (i) *If* p *does not divide* n *then* $\dim(J^{(f,q)}) = \frac{(p^r - p^{r-1})(n-1)}{2}$.
If q *divides* n *then* $\dim(J^{(f,q)}) = \frac{(p^r - p^{r-1})(n-2)}{2}$;

(ii) *If p does not divide n then there is an $K(\zeta_q)$-isogeny $J(C_{f,q}) \to J(C_{f,q/p}) \times J^{(f,q)}$.*

(iii) *If p does not divide n and $\zeta \in K$ then the Galois modules $V_{f,p}$ and*

$$(J^{(f,q)})^{\delta_q} := \{z \in J^{(f,q)}(K_a) \mid \delta_q(z) = z\}$$

are isomorphic.

Proof. Clearly, we may assume that $\zeta \in K$. It follows from Remark 4.3 that we may assume that p does *not* divide n. Clearly, the assertion (ii) implies the assertion (i). Further we will prove the assertions (ii) and (iii).

Let us consider the curve

$$C_{f,q/p} : y_1^{q/p} = f(x_1)$$

and a regular surjective map

$$\pi_1 : C_{f,q} \to C_{f,q/p}, \quad x_1 = x, y_1 = y^p.$$

Clearly,

$$\pi_1 \delta_q = \delta_{q/p} \pi_1.$$

By Albanese functoriality, π_1 induces a certain surjective homomorphism of jacobians $J(C_{f,q}) \twoheadrightarrow J(C_{f,q/p})$ which we continue to denote by π_1. Clearly, the equality $\pi_1 \delta_q = \delta_{q/p} \pi_1$ remains true in $\mathrm{Hom}(J(C_{f,q}), J(C_{f,q/p}))$. By Lemma 4.8,

$$\mathcal{P}_{q/p}(\delta_{q/p}) = 0 \in \mathrm{End}(J(C_{f,q/p})).$$

It follows from Lemma 4.10 that

$$\pi_1(J^{(f,q)}) = 0.$$

It follows that $\dim(J^{(f,q)})$ does not exceed

$$\dim(J(C_{f,q})) - \dim(J(C_{f,q/p})) = \frac{(p^r-1)(n-1)}{2} - \frac{(p^{r-1}-1)(n-1)}{2} = \frac{(p^r - p^{r-1})(n-1)}{2}.$$

By definition of $J^{(f,q)}$, for each divisor $D = \sum_{P \in B} a_P(P)$ the linear equivalence class of

$$p^{r-1}D = \sum_{P \in B} p^{r-1} a_P(P)$$

lies in $(J^{(f,q)})^{\delta_q} \subset J^{(f,q)}(K_a) \subset J(C_{f,q})(K_a)$. It follows from Lemma 4.7 that the class of $p^{r-1}D$ is zero if and only if all $p^{r-1}a_P$ are divisible by $q = p^r$, i.e. all a_P are divisible by p. This implies that the set of linear equivalence classes of $p^{r-1}D$ is a Galois submodule isomorphic to $V_{f,p}$. We need to prove that $(J^{(f,q)})^{\delta_q} = V_{f,p}$.

Recall that $J^{(f,q)}$ is δ_q-invariant and the restriction of δ_q to $J^{(f,q)}$ satisfies the qth cyclotomic polynomial. This allows us to define the homomorphism

$$\mathbf{Z}[\zeta_q] \to \mathrm{End}(J^{(f,q)})$$

which sends 1 to the identity map and ζ_q to δ_q. Let us put

$$E = \mathbf{Q}(\zeta_q), \emptyset = \mathbf{Z}[\zeta_q] \subset \mathbf{Q}(\zeta_q) = E.$$

It is well-known that $\emptyset$ is the ring of integers in E,

$$\lambda = (1-\zeta_q)\mathbf{Z}[\zeta_q] = (1-\zeta_q)\emptyset$$

is a maximal ideal in $\emptyset$ with $\emptyset/\lambda = \mathbf{F}_p$ and $\emptyset \otimes \mathbf{Z}_p = \mathbf{Z}_p[\zeta_q]$ is the ring of integers in the field $\mathbf{Q}_p(\zeta_q)$. Notice also that $\emptyset \otimes \mathbf{Z}_p$ coincides with the completion $\emptyset_\lambda$ of $\emptyset$ with respect to λ-adic topology and $\emptyset_\lambda/\lambda\emptyset_\lambda = \emptyset/\lambda = \mathbf{F}_p$.

It follows (see [7]) that

$$d = \frac{2\dim(J^{(f,q)})}{E:\mathbf{Q}]} = \frac{2\dim(J^{(f,q)})}{p^r - p^{r-1}}$$

is a positive integer and the $\mathbf{Z}_p$-Tate module $T_p(J^{(f,q)})$ is a free $\emptyset_\lambda$-module of rank d. It follows that $T_p(J^{(f,q)}) \otimes_{\emptyset_\lambda} \mathbf{F}_p$ is a d-dimensional vector space. On the other hand, clearly

$$(J^{(f,q)})^{\delta_q} = \{u \in J^{(f,q)}(K_a) \mid (1-\delta_p)(u) = 0\} = J^{f,q}_\lambda = T_p(J^{f,q}) \otimes_{\emptyset_\lambda} \mathbf{F}_p.$$

Since $(J^{(f,q)})^{\delta_q}$ contains $(n-1)$-dimensional $\mathbf{F}_p$-vector space $V_{f,p}$,

$$d \geq n-1.$$

This implies that

$$2\dim(J^{(f,q)}) = d(p^r - p^{r-1}) \geq (n-1)(p^r - p^{r-1})$$

and therefore

$$\dim(J^{(f,q)}) \geq \frac{(n-1)(p^r - p^{r-1})}{2}.$$

But we have already seen that

$$\dim(J^{(f,q)}) \leq \frac{(n-1)(p^r - p^{r-1})}{2}.$$

This implies that

$$\dim(J^{(f,q)}) = \frac{(n-1)(p^r - p^{r-1})}{2}.$$

It follows that $d = n-1$ and therefore

$$(J^{(f,q)})^{\delta_q} = V_{f,p}.$$

□

Corollary 4.12. *If p does not divide n then there is a $K(\zeta_q)$-isogeny $J(C_{f,q}) \to J(C_{f,p}) \times \prod_{i=2}^{r} J^{(f,p^i)} = \prod_{i=1}^{r} J^{(f,p^i)}$.*

Proof. Combine Corollary 4.11(ii) and Remark 4.9 with easy induction by r. □

Remark 4.13. Suppose that p does not divide n and consider the induced linear operator

$$\delta_q^* : \Omega^1(J^{(f,q)}) \to \Omega^1(J^{(f,q)}).$$

It follows from Theorem 3.9 combined with Remark 4.6 that its spectrum consists of primitive qth roots of unity ζ^{-i} $(1 \le i < q)$ with $\left[\frac{ni}{q}\right] > 0$ and the multiplicity of ζ^{-i} equals $\left[\frac{ni}{q}\right]$.

Theorem 4.14. *Suppose that $n \ge 5$ is an integer. Let p be a prime, $r \ge 1$ an integer and $q = p^r$. Suppose that p does not divide n. Suppose that K is a field of characteristic different from p containing a primitive qth root of unity ζ, Let $f(x) \in K[x]$ be a separable polynomial of degree n and $\mathrm{Gal}(f)$ its Galois group. Suppose that the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. Then the image $\emptyset$ of*

$$\mathbf{Z}[\delta_q] \to \mathrm{End}(J^{(f,q)})$$

is isomorphic to $\mathbf{Z}[\zeta_q]$ and enjoys one of the following two properties.

(i) *$\emptyset$ is a maximal commutative subring in $\mathrm{End}(J^{(f,q)})$;*
(ii) *$\mathrm{char}(K) > 0$ and the centralizer of $\emptyset \otimes \mathbf{Q} \cong \mathbf{Q}(\zeta_q)$ in $\mathrm{End}^0(J^{(f,q)})$ is a central simple $(n-1)^2$-dimensional $\mathbf{Q}(\zeta_q)$-algebra.*

Proof. Clearly, $\emptyset$ is isomorphic to $\mathbf{Z}[\zeta_q]$. Let us put $\lambda = (1-\zeta_q)\mathbf{Z}[\zeta_q]$. By Lemma 4.11(iii), the Galois module $(J^{(f,q)})^{\delta_q} = J_\lambda^{(f,q)}$ is isomorphic to $V_{f,p}$. Applying Theorem 3.7, we conclude that either (ii) holds true or one of the following conditions hold:

(a) $\emptyset$ is a maximal commutative subring in $\mathrm{End}(J^{(f,q)})$;
(b) $\mathrm{char}(K) = 0$ and there exist a $\frac{\varphi(q)}{2}$-dimensional abelian variety Z over K_a, an embedding $\mathbf{Q}(\zeta_q) \hookrightarrow \mathrm{End}^0(Z)$ and a $\mathbf{Q}(\zeta_q)$-equivariant isogeny $\psi : Z^{n-1} \to J^{(f,q)}$.

Clearly, if (a) is fulfilled then we are done

If $q = p$ and $\mathrm{char}(K) = 0$ then it is known [17], [19, Th. 5.3] that (a) is fulfilled.

So further we may assume that (b) holds true. In particular, $\mathrm{char}(K) = 0$. We may also assume that $q > p$. In order to finish the proof, we need to arrive to a contradiction. Clearly, ψ induces an isomorphism

$$\psi^* : \Omega^1((J^{(f,q)})) \cong \Omega^1(Z^{n-1})$$

that commutes with the action of $\mathbf{Q}(\zeta_q)$. (Here again we use that $\mathrm{char}(K) = 0$.) Since

$$\dim\Omega^1(Z) = \dim(Z) = \frac{\varphi(q)}{2}.$$

the linear operator in $\Omega^1(Z)$ induced by ζ_q has, at most, $\frac{\varphi(q)}{2}$ distinct eigenvalues. It follows that the linear operator in $\Omega^1(Z^{n-1}) = \Omega^1(Z)^{n-1}$ induced by ζ_q also has, at most, $\frac{\varphi(q)}{2}$ distinct eigenvalues. This implies that the linear operator δ_q^* in $\Omega^1((J^{(f,q)}))$ also has, at most, $\frac{\varphi(q)}{2}$ distinct eigenvalues. Recall that the eigenvalues of δ_q^* are primitive qth roots of unity ζ^{-i} with

$$1 \le i < q, (i,p) = 1, \left[\frac{ni}{q}\right] > 0.$$

Clearly, the inequality $\left[\frac{ni}{q}\right] > 0$ means that $ni \ge q$, i.e.

$$i \ge \frac{q}{n} \ge \frac{q}{5}.$$

So, in order to get a desired contradiction, it suffices that the cardinality of the set of integers

$$B := \left\{ i \mid \frac{q}{5} \le i < q = p^r, (i,p) = 1 \right\}$$

is strictly greater than $(p-1)p^{r-1}/2$. Indeed, clearly, $\frac{p}{5} < \frac{p-1}{2}$ and

$$\#(B) > \varphi(q) - \frac{q}{5} = (p-1)p^{r-1} - \frac{p^{r-1}p}{5} = (p-1-\frac{p}{5})p^{r-1} > \frac{p-1}{2}p^{r-1}.$$

□

Corollary 4.15. *Suppose that $n \ge 5$ is an integer. Let p be a prime, $r \ge 1$ an integer and $q = p^r$. Assume in addition that either p does not divide n or $q \mid n$ and $(n,q) \ne (5,5)$. Let K be a field of characteristic different from p, Let $f(x) \in K[x]$ be an irreducible separable polynomial of degree n such that $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$. Then the image $\emptyset$ of*

$$\mathbf{Z}[\delta_q] \to \mathrm{End}(J^{(f,q)})$$

is isomorphic to $\mathbf{Z}[\zeta_q]$ and enjoys one of the following two properties.

- *(i)] $\emptyset$ is a maximal commutative subring in $\mathrm{End}(J^{(f,q)})$;*

- *(ii)]* $\mathrm{char}(K) > 0$ *and the centralizer of* $\emptyset \otimes \mathbf{Q} \cong \mathbf{Q}(\zeta_q)$ *in* $\mathrm{End}^0(J^{(f,q)})$ *is a central simple* $(n-1)^2$*-dimensional* $\mathbf{Q}(\zeta_q)$*-algebra.*

Proof. If p divides n then $n > 5$ and therefore $n - 1 \ge 5$. By Remark 4.3, we may assume that p does not divide n. If we replace K by $K(\zeta)$ then still $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$. By Remark 4.1 if $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$ then the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. One has only apply Theorem 4.14. □

Theorem 4.16. *Suppose* $n \ge 4$ *and* p *does not divide* n*. Assume also that* $\mathrm{char}(K) = 0$ *and* $\mathbf{Q}[\delta_q]$ *is a maximal commutative subalgebra in* $\mathrm{End}^0(J^{(f,q)})$*. Then* $\mathrm{End}^0(J^{(f,q)}) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}(\zeta_q)$ *and therefore* $\mathrm{End}(J^{(f,q)}) = \mathbf{Z}[\delta_q] \cong \mathbf{Z}[\zeta_q]$*. In particular,* $J^{(f,q)}$ *is an absolutely simple abelian variety.*

Proof. Let $\mathfrak{C} = \mathfrak{C}_{J^{(f,p)}}$ be the center of $\mathrm{End}^0(J^{(f,p)})$. Since $\mathbf{Q}[\delta_q]$ is a maximal commutative, $\mathfrak{C} \subset \mathbf{Q}[\delta_q]$.

Replacing, if necessary, K by its subfield (finitely) generated over $\mathbf{Q}$ by all the coefficients of f, we may assume that K (and therefore K_a) is isomorphic to a subfield of the field $\mathbf{C}$ of complex numbers. So, $K \subset K_a \subset \mathbf{C}$. We may also assume that $\zeta = \zeta_q$ and consider $J^{(f,q)}$ as complex abelian variety.

Let $\Sigma = \Sigma_E$ be the set of all field embeddings $\sigma : E = \mathbf{Q}[\delta_q] \hookrightarrow \mathbf{C}$. We are going to apply Theorem 2.2 to $Z = J^{(f,q)}$ and $E = \mathbf{Q}[\delta_q]$. In order to do that we need to get some information about the multiplicities

$$n_\sigma = n_\sigma(Z, E) = n_\sigma(J^{(f,q)}, \mathbf{Q}[\delta_q]).$$

Remark 2.1 allows us to do it, using the action of $\mathbf{Q}[\delta_q]$ on the space $\Omega^1(J^{(f,q)})$ of differentials of the first kind on $J^{(f,q)}$.

In other words, $\Omega^1(J^{(f,q)})_\sigma$ is the eigenspace corresponding to the eigenvalue $\sigma(\delta_q)$ of δ_q and n_σ is the multiplicity of the eigenvalue $\sigma(\delta_q)$.

Let $i < q$ be a positive integer that is not divisible by p and $\sigma_i : \mathbf{Q}[\delta_p] \hookrightarrow \mathbf{C}$ be the embedding which sends δ_p to ζ^{-i}. Clearly, for each σ there exists precisely one i such that $\sigma = \sigma_i$. Clearly, $\Omega^1(J^{(f,q)})_{\sigma_i}$ is the eigenspace of $\Omega^1(J^{(f,q)})$ attached to the eigenvalue ζ^{-i} of δ_q. Therefore n_{σ_i} coincides with the multiplicity of the eigenvalue ζ^{-i}. It follows from Remark 4.13 that

$$n_{\sigma_i} = \left[\frac{ni}{q}\right].$$

Now the assertion of the Theorem follows from Corollary 2.3 applied to $E = \mathbf{Q}(\zeta_q) \cong \mathbf{Q}[\delta_q]$. □

Combining Corollary 4.15 and 4.16, we obtain the following statement.

Theorem 4.17. *Let p be a prime, r a positive integer, $q = p^r$ and K a field of characteristic zero. Suppose that $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$. Assume also that either p does not divide n or q divides n. Then $\mathrm{End}^0(J^{(f,q)}) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}(\zeta_q)$ and therefore $\mathrm{End}(J^{(f,q)}) = \mathbf{Z}[\delta_q] \cong \mathbf{Z}[\zeta_q]$. In particular, $J^{(f,q)}$ is an absolutely simple abelian variety.*

Combining Theorem 4.16 amd Corollary 4.14, we obtain the following statement.

Theorem 4.18. *Let p be a prime, r a positive integer, $q = p^r$ and K a field of characteristic zero. Let $f(x) \in K[x]$ be an polynomial of degree $n \geq 5$. Assume also that p does not divide n and the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. Then $\mathrm{End}^0(J^{(f,q)}) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}(\zeta_q)$ and therefore $\mathrm{End}(J^{(f,q)}) = \mathbf{Z}[\delta_q] \cong \mathbf{Z}[\zeta_q]$. In particular, $J^{(f,q)}$ is an absolutely simple abelian variety.*

5. Jacobians and their endomorphism rings

Throughout this section we assume that K is a field of characteristic zero. Recall that K_a is an algebraic closure of K and $\zeta \in K_a$ is a primitive qth root of unity. Suppose $f(x) \in K[x]$ is a polynomial of degree $n \geq 5$ without multiple roots, $\mathfrak{R}_f \subset K_a$ is the set of its roots, $K(\mathfrak{R}_f)$ is its splitting field. Let us put

$$\mathrm{Gal}(f) = \mathrm{Gal}(K(\mathfrak{R}_f)/K) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

Let r be a positive integer. Recall (Corollary 4.12) that if p does not divide n then there is a $K(\zeta_{p^r})$-isogeny $J(C_{f,p^r}) \to \prod_{i=1}^r J^{(f,p^i)}$. Applying Theorem 4.18 to all $q = p^i$, we obtain the following assertions.

Theorem 5.1. *Let p be a prime, r a positive integer, $q = p^r$ and K a field of characteristic zero. Let $f(x) \in K[x]$ be an polynomial of degree $n \geq 5$. Assume also that p does not divide n and the $\mathrm{Gal}(f)$-module $V_{f,p}$ is very simple. Then*

$$\mathrm{End}^0(J(C_{f,q})) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^r \mathbf{Q}(\zeta_{p^i}).$$

Theorem 5.2. *Let p be a prime, r a positive integer and K a field of characteristic zero. Suppose that $f(x) \in K[x]$ is an irreducible polynomial of degree $n \geq 5$ and $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$. Assume also that either p does not divide n or*

$$\mathrm{End}^0(J(C_{f,q})) = \mathbf{Q}[\delta_q] \cong \mathbf{Q}[t]/\mathcal{P}_q(t)\mathbf{Q}[t] = \prod_{i=1}^r \mathbf{Q}(\zeta_{p^i}).$$

Proof. The existence of the isogeny $J(C_{f,q}) \to \prod_{i=1}^r J^{f,(p^i)}$ combined with Theorem 4.17 implies that the assertion holds true if p does not divide n. If q divides n then Remark 4.3 allows us to reduce this case to the already proven case when p does not divide $n-1$. □

Example 5.3. Suppose $L = \mathbf{C}(z_1, \cdots, z_n)$ is the field of rational functions in n independent variables $z_1, \cdots, z_n$ with constant field $\mathbf{C}$ and $K = L^{\mathbf{S}_n}$ is the subfield of symmetric functions. Then $K_a = L_a$ and

$$f(x) = \prod_{i=1}^{n}(x - z_i) \in K[x]$$

is an irreducible polynomial over K with Galois group $\mathbf{S}_n$. Let Let $q = p^r$ be a power of a prime p. Let C be a smooth projective model of the K-curve $y^q = f(x)$ and $J(C)$ its jacobian. It follows from Theorem 5.2 that if $n \geq 5$ and either p does not divide n or q divides n then the algebra of L_a-endomorphisms of $J(C)$ is $\prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

Example 5.4. Let $h(x) \in \mathbf{C}[x]$ be a *Morse polynomial* of degree $n \geq 5$. This means that the derivative $h'(x)$ of $h(x)$ has $n-1$ distinct roots $\beta_1, \cdots \beta_{n-1}$ and $h(\beta_i) \neq h(\beta_j)$ while $i \neq j$. (For example, $x^n - x$ is a Morse polynomial.) Let $K = \mathbf{C}(z)$ be the field of rational functions in variable z with constant field $\mathbf{C}$ and K_a its algebraic closure. Then a theorem of Hilbert ([13, theorem 4.4.5, p. 41]) asserts that the Galois group of $h(x) - z$ over $k(z)$ is $\mathbf{S}_n$. Let $q = p^r$ be a power of a prime p. Let C be a smooth projective model of the K-curve $y^q = h(x) - z$ and $J(C)$ its jacobian. It follows from Theorem 5.2 that if either p does not divide n or q divides n then the algebra of K_a-endomorphisms of $J(C)$ is $\prod_{i=1}^r \mathbf{Q}(\zeta_{p^i})$.

References

[1] I. N. Herstein, Noncommutative rings. John Wiley and Sons, 1968.

[2] J. K. Koo, *On holomorphic differentials of some algebraic function field of one variable over* C. Bull. Austral. Math. Soc. **43** (1991), 399–405.

[3] S. Lang, Abelian varieties, Springer Verlag 1983.

[4] B. Moonen and Yu. G. Zarhin, *Weil classes on abelian varieties*. J. reine angew. Math. **496** (1998), 83–92.

[5] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*. Proc. London Math. Soc. (3) **41** (1980), 1–20.

[6] D. Mumford, Abelian varieties, 2nd edn (Oxford University Press, 1974).

[7] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*. Amer. J. Math. 98 (1976), 751–804.

[8] K. Ribet, *Hodge classes on certain abelian varieties*. Amer. J. Math. **105** (1983), 523–538.

[9] B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*. J. reine angew. Math. **488** (1997), 141–188.

[10] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*. Math. Ann. **310** (1998), 447–471.

[11] I. Schur, *Gleichungen ohne Affect*. Sitz. Preuss. Akad. Wiss. 1930, Physik-Math. Klasse 443–449 (=Ges. Abh. III, 191–197).

[12] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves. AK Peters, Wellesley, 1998.

[13] J.-P. Serre, Topics in Galois Theory, Jones and Bartlett Publishers, 1992.

[14] C. Towse, *Weierstrass points on cyclic covers of the projective line*. Trans. Amer. Math. Soc. **348** (1996), 3355-3377.

[15] Yu. G. Zarhin, *Weights of simple Lie algebras in the cohomology of algebraic varieties*. Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), 264–304; English translation: Math. USSR Izv. **24** (1985), 245 - 281.

[16] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **7** (2000), 123–132.

[17] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*. In: Moduli of abelian varieties (eds. C. Faber, G. van der Geer and F. Oort). Progress in Math., vol. **195** (Birkhäuser, 2001), pp. 473–490.

[18] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication in positive characteristic*. Math. Res. Letters **8** (2001), 429–435.

[19] Yu. G. Zarhin, *Cyclic covers of the projective line, their jacobians and endomorphisms*. J. reine angew. Math. **544** (2002), 91–110.

[20] Yu. G. Zarhin, *Endomorphism rings of certain jacobians in finite characteristic*. Matem. Sbornik **193** (2002), issue 8, 39–48; Sbornik Math., 2002, **193** (8), 1139-1149.

[21] Yu. G. Zarhin, *Very simple* 2*-adic representations and hyperelliptic jacobians*. Moscow Math. J. **2** (2002), issue 2, 403-431.

[22] Yu. G. Zarhin, *Homomorphisms of hyperelliptic jacobians*. In: Number Theory, Algebra, and Algebraic geometry (Shafarevich Festschrift), Proc. Steklov Math. Institute **241** (2003), 90–104; e-print: http://arXiv.org/abs/math.NT/0301173 .

[23] Yu. G. Zarhin, *The endomorphism rings of jacobians of cyclic covers of the projective line*. Math. Proc. Cambridge Philos. Soc. **136** (2004), to appear.

[24] Yu. G. Zarhin, *Very simple representations: variations on a theme of Clifford*. In: Galois Theory Conference Proceedings (H. Völklein, ed.), Developments in Math., Kluwers, to appear; e-print: http://front.math.ucdavis.edu/math.GR/0209083 .

[25] Yu. G. Zarhin, *Non-supersingular hyperelliptic jacobians*. e-print: http://front.math.ucdavis.edu/math.AG/0311137 .

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address: zarhin@math.psu.edu